Information technology and systems report

Governance

The effective management of information, information technology (IT) and information systems (IS) is key to achieving our strategic objectives, particularly in delivering excellent client service and supporting long-term investment outperformance. The Board aims to represent the interests of all stakeholders in delivering a successful and sustainable business. Accordingly, the Board is accountable for governing the ethical and effective application of resources toward the achievement of strategic outcomes to create value for stakeholders.

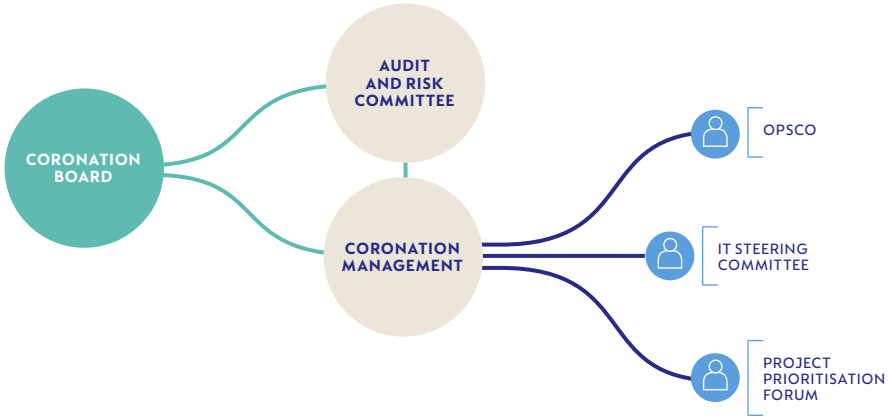
IT and IS at Coronation are viewed as key enablers of the Group's strategic objectives, and as such, require robust governance.

The Group has identified the following as key technology and information governance objectives:

- Monitoring the alignment of short-, medium- and long-term strategies of the business and technology;
- Maintaining formalised IT governance at Coronation, aligned to existing corporate governance structures and leading practices;
- Monitoring the integrity and availability of technology and information to meet business needs in a timely manner;
- Developing and maintaining appropriate organisational structures, relationships, frameworks and processes to support IT governance;
- Measuring and managing the cost expended and the value received from technology;
- Managing technology resources and assets, including information, in an efficient and effective manner, such that the value derived from these resources is maximised;
- Safeguarding technology resources and information;
- Monitoring adherence to legislative requirements and other guidance as it pertains to IT management relevant to the Group, including but not limited to King IV™ Control Objectives for Information and Related Technologies (COBIT); the Information Technology Infrastructure Library (ITIL); and the International Organisation for Standardisation 27000 series supporting information security (ISO 27000);
- Establishing appropriate polices and frameworks pertaining to managing IT across the business and monitoring adherence thereto; and
- Establishing performance criteria aligned with operational expectations and periodic measurement of actual versus desired performance levels.

The Board has delegated the responsibility for the governance of IT to Coronation management. Management approves the direction for how IT should be managed and is supported by the Operations Committee (OPSCO), the IT Steering Committee and the Project Prioritisation Forum.

In addition, the Board has mandated the Audit and Risk Committee to oversee the adequate and effective risk management and system of internal control, including those pertaining to technology. The organisational and governance structure is illustrated in the following visual.



We also set up dedicated committees to deal with specific technology projects.

Party	Role and responsibility
Coronation Board	› Sets strategic goals and objectives for the business including IT-related goals and objectives › Evaluates and approves significant IT-related initiatives › Exercises ongoing oversight of IT management › Evaluates the effectiveness of the Company's IT arrangements, including outsourced services, in achieving strategic objectives › Monitors implementation of significant technology initiatives/projects › Monitors the management of technology-related risks, including cyber risk, with the support of the Audit and Risk Committee
Audit and Risk Committee	› Monitors the management of IT-related risks, including cyber risk › Oversees technology-, IS- and information-related assurance
Management	› Establish the target business and operating model to achieve strategic goals established by the Board › Responsible for implementation and execution of effective IT management within the business › Approve significant IT-related initiatives prior to seeking the Board approval to implement › Oversee major IT projects
OPSCO	› Drives implementation of IT-related projects › Recommends technology-related projects to executives based on strategic goals and objectives › Oversees end-user acceptance of technology › Responsible for the operational management of IT
IT Steering Committee	› Drives implementation of appropriate technology infrastructure to support business and objectives › Advises on technology-related risks faced by the business › Acts as an adviser to the business in respect of IT
Project Prioritisation Forum	› Prioritises and optimises efficient delivery of approved projects

Key areas of focus in 2018

To further our strategic objective of excellent client service, we maintained our drive to deliver on our key projects, all of which ultimately will contribute to an improved client experience and a reduction in risk.

During the period, the major focus areas were as follows:

Implementing our new administration model

As communicated to the market in July 2017, we determined that significant changes were required to our outsourced administration model to enable us to continue to provide our clients with world-class services. The most significant elements of the new model are as follows:

- Asset administration services
  - Consolidation of our outsourced administration services with a single service provider
  - Insourcing of certain functions which were previously outsourced
- Transfer agency
  - Creation of a new, independent black-owned transfer agency business

Over the course of the last 18 months, significant IT resources were dedicated to establishing the new model, specifically:

- **The transfer of administration services to JP Morgan and establishing a new in-house middle-office function**

  Effective 1 July 2018, we successfully completed the transfer of the asset administration of our domestic products to JP Morgan and implemented our new in-house 'middle office' function which includes matching and settlement, trade support, corporate actions processing, and proxy voting processing.

  During the implementation of the project, we identified an opportunity to enhance our data management through the implementation of the foundations of a meta-data management solution using best of breed industry technology. Significant technology and operational resources were devoted to ensuring the on-time delivery of all services required to complete our implementation on time and in line with what we have previously communicated to the market.

- **The migration of our transfer agency services**

  As part of our new administration model, Coronation has supported the creation of a new black-owned transfer agency business, IntIA. Over the last year, significant resources, in terms of both people and technology, have been dedicated to implement and establish this new venture. Migration to the new transfer agency service was completed in November 2018. We expect that our contribution to the establishment of InTIA will result not only in a great experience for our clients but also in the achievement of the objectives of B-BBEE through the distribution of InTIA profits to black beneficiaries.

- **The management of technology risks**

  Coronation's key technology risks are detailed on → *pages 94 to 95*. During the past year, there was no material breach of our IT and IS security processes to manage these risks. We measure the value added by our IT strategy and investments against the following benchmarks:

  - Improvements in client service and meeting the evolving needs of clients;
  - Derisking of the business;
  - The scalability and flexibility of systems;
  - Operational efficiencies and cost savings; and
  - Platform stability .

  Outcomes are measured through active monitoring and feedback from clients and intermediaries. Our evaluation of our performance against these benchmarks is favourable. We remain committed to ensuring that they are met through our efficient delivery of sustainable, scalable technology solutions.

IT risk management

We consider technology risks as part of our overall risk assessment. These risks are incorporated in an annual operational risk assessment and material IT/IS risks are escalated to the key risk register which is submitted to the Audit and Risk Committee. The Committee also reviews regular reports on IT and IS risk. Key technology risks are detailed below:

Risk	Mitigation strategies
Security of information	We monitor and protect security of information through various measures, including file tracking and monitoring, data loss prevention software, access controls, approval processes and backup controls. Coronation's SOC monitors these measures. Coronation has implemented software to identify cyber attacks in real time. A summary of these attempts is reported to the Audit and Risk Committee.
Disaster recovery and business continuity	Coronation has an established Business Continuity and Disaster Recovery Plan. Disaster recovery tests are conducted annually, and the results are reviewed by the Audit and Risk Committee. An integral component of our business continuity planning involves the assessment of potential disruptive events that could affect normal working operations. These scenarios are workshopped with the relevant business heads to agree on the most appropriate response that will ensure business continuity.
Cyber security risk	This includes the loss of data confidentiality, availability and integrity as a result of unauthorised access to systems. Cyber risk is holistically managed across people, process and technology. This includes enforcing appropriate policies, ongoing employee awareness and employing technology to prevent and/or detect potential or actual threats to the security of the environment. Vulnerability management occurs on an ongoing basis on both the server and desktop environments. In addition, independent subject matter experts perform penetration testing at regular intervals, and the implementation of recommendations are closely monitored.
Third-party supplier risk	A significant number of operational procedures have been designed to exercise adequate and effective oversight over these third parties. These operational processes are audited annually. In addition, periodic due diligence is performed on material service providers in terms of a defined Service Provider Framework. Feedback on IT due diligence performed on material service providers is distributed to the audit and risk committee. Third-party ISAE 3402 reports are regularly obtained and distributed to the Chairperson of the Audit and Risk Committee. Coronation reviews daily diagnostic reports and incident logs from service providers.
Duplicate and inconsistent data	Data have been migrated to a new data warehouse which has improved control functionality and data governance, as well as ownership reporting capabilities.
Failure to resolve data validation and integration errors between internal and external systems accurately and in a timely manner	We has a number of procedures in place for the early detection and resolution of variances, including automated and manual reconciliations that are performed to detect variances, as well as an alert system on automated errors.
Unavailability of cloud-based solutions	Redundant connectivity has been built into email, internet and telephone lines. Strong relationships are maintained with vendors, which is monitored through constant evaluation. In addition, clear escalation paths are defined and cloud due diligence assessments are performed.
Inability to recruit IS employees with the relevant skills and experience	Coronation has talent management initiatives (detailed on → *pages 52 to 54*) to attract highly skilled employees. In the event that it is not possible to recruit IS employees of suitable skills and experience, an insourcing arrangement will be entered into.

Risk	Mitigation strategies
Failure to upgrade or replace key systems and infrastructure to meet changing business needs/ business priorities	An information systems strategy is in place, which governs the replacement strategy of key systems and the achievement of business requirements. Furthermore, IT and IS report to the COO, which facilitates alignment between business and technology.
Failure to secure client and other confidential data on mobile devices	A Mobility and Bring Your Own Device (BYOD) Policy is in place, enforcing password controls on mobile devices. Our systems also have the ability to remotely clear and secure mobile phones.

The IT general control environment is annually assured in accordance with ISAE 3402. In addition, specific IT/IS reviews are performed by PricewaterhouseCoopers. The results of these reviews are reported to the Audit and Risk Committee.

Future focus

- Enhancing and extracting additional efficiencies from the new services related to JP Morgan outsourcing and middle office.
- The wider roll out of CRM systems, improved automation and workflow.
- Implementation of solutions to address regulatory changes required by the FIC.
- Effective management of software vendors.
- The governance, management and security of data will continue to be a priority.
- Implementing a Protection of Personal Information (POPI) Framework.